

## **Communication Systems and System Support**

### **Service Name: Virtual Private Network (VPN) Individual User**

**1. Service Description:** Fort Detrick DOIM provides VPN secure access to the Fort Detrick Local Area Network (LAN). A VPN provides a means for a Fort Detrick user of Ft. Detrick services to access the services from a remote location over a secure channel. This is done with a method of authenticating the user and encapsulating the data as it traverses the network, allowing it to bypass most access lists. The access method used is independent of the VPN service. The base access method might be TSACS, a cable service from a local provider, or some other dial-up method. VPN is a security augmentation to the base access method. User authentication identifies the user to the VPN service provider. By encapsulating user data it is “sealed”, so it passes across the networks between the users’ PC and the VPN service provider without causing harm or being interrupted along the way. In effect the VPN service provider is vouching for the user and the users’ network activities.

### **2. DOIM Responsibilities:**

- a. Engineer and operate a VPN environment supported by hardware and software that will permit authorized users to access their Fort Detrick Network Infrastructure resources from approved remote locations and authorized equipment; maintain a list of any disapproved Internet Service Providers based on ACERT or other official advisories; issue, manage, and maintain VPN accounts and authorizations; and implement and configure required hardware and/or software for the approved remote equipment.
- b. Perform a security scan of the Receiver personal computer
- c. Provide VPN account
- d. Provide VPN Client
- e. Provide hardware which the user will connect to through the use of broadband or dial-up access while TDY or working off post from Fort Detrick
- f. Provide security requirements, operational guidelines, and user authentication.

### **3. Customer Responsibilities:**

- a. Provide Government Furnished Equipment (GFE) for connection to Fort Detrick LAN via VPN.
- b. Make pc available to the Supplier for security scan and installation of the VPN client.
- c. Arrange for reimbursement of the Fort Detrick DOIM for the cost of services provided.
- d. Designate authorized users and coordinate with the Fort Detrick DOIM Information Support Division for the implementation and configuration of required hardware and/or software to support authorizations.
- e. Use VPN for official Government business only
- f. Run latest Anti-Virus software/latest security updates
- g. NOT share user authentication information

- h. Select and arrange for payment of acceptable Internet Service Provider (ISP).
- i. Install, manage, and maintain any software or hardware required by the ISP for access.
- j. Have GFE scanned for vulnerabilities according to local security policy according to local security policy. (EXAMPLE: quarterly)
- k. Coordinate through the Fort Detrick DOIM Customer Support Center (CSC) for installation and configuration of VPN hardware and/or software on approved remote equipment subsequent to verification of correct operation of services from the ISP.
- l. Recognize that the VPN establishes the remote equipment as an extension of the Fort Detrick Network Infrastructure subject to all US Government, DOD, DA, Fort Detrick, and organizational rules and regulations that apply to hardware, software, and use of those Network facilities.

**4. Questions/Contact Information:** If you have any questions or would like to obtain this service, please contact your Customer Account Manager (CAM) or check the DOIM web site at: <http://doim.detrick.army.mil>. If you do not know your CAM or your organization does not have a CAM assigned please contact the DOIM Help Desk at 301-619-2049 or via email at: [usagdoimhelpdesk@amedd.army.mil](mailto:usagdoimhelpdesk@amedd.army.mil).